ODP Ltr

ILLEGIB

ODP-81-383
24 March 1981

[redacted]

MEMORANDUM FOR: Information Handling Systems Architect
Chairman, Agency-wide Committee on Software Engineering Standards
OC ADP Control Officer
Deputy Director for Processing, ODP
Chief, Engineering Division, ODP

ILLEGIB

STAT FROM : [redacted]
Chief, Management Staff, ODP

SUBJECT : Proposed Revision to FIPS 71, entitled "Advanced Data Communication Control Procedures"

1. Revisions to Federal Information Processing Standard 71, entitled "Advanced Data Communication Control Procedures," are being proposed to make FIPS 71 more clearly consistent with the revised Federal Standard 1003 being processed by the General Services Administration and the National Communications System. A copy of the proposed revisions to FIPS 71 is attached. (FIPS 71 is available for review in the ODP Management Staff, Room 2D0109, Headquarters; FIPS 78, Guideline for Implementing Advanced Data Communication Control Procedures, referenced in the attached is unfortunately not available at this time.)

2. We ask that you provide comments on the revision by 1 June 1981. Comments on any requirements not provided for in this proposed revised standard would be most helpful. Please also comment on the cost impact as well as any benefits that you anticipate will result from the implementation of this proposed revised standard. If you have any questions, please contact

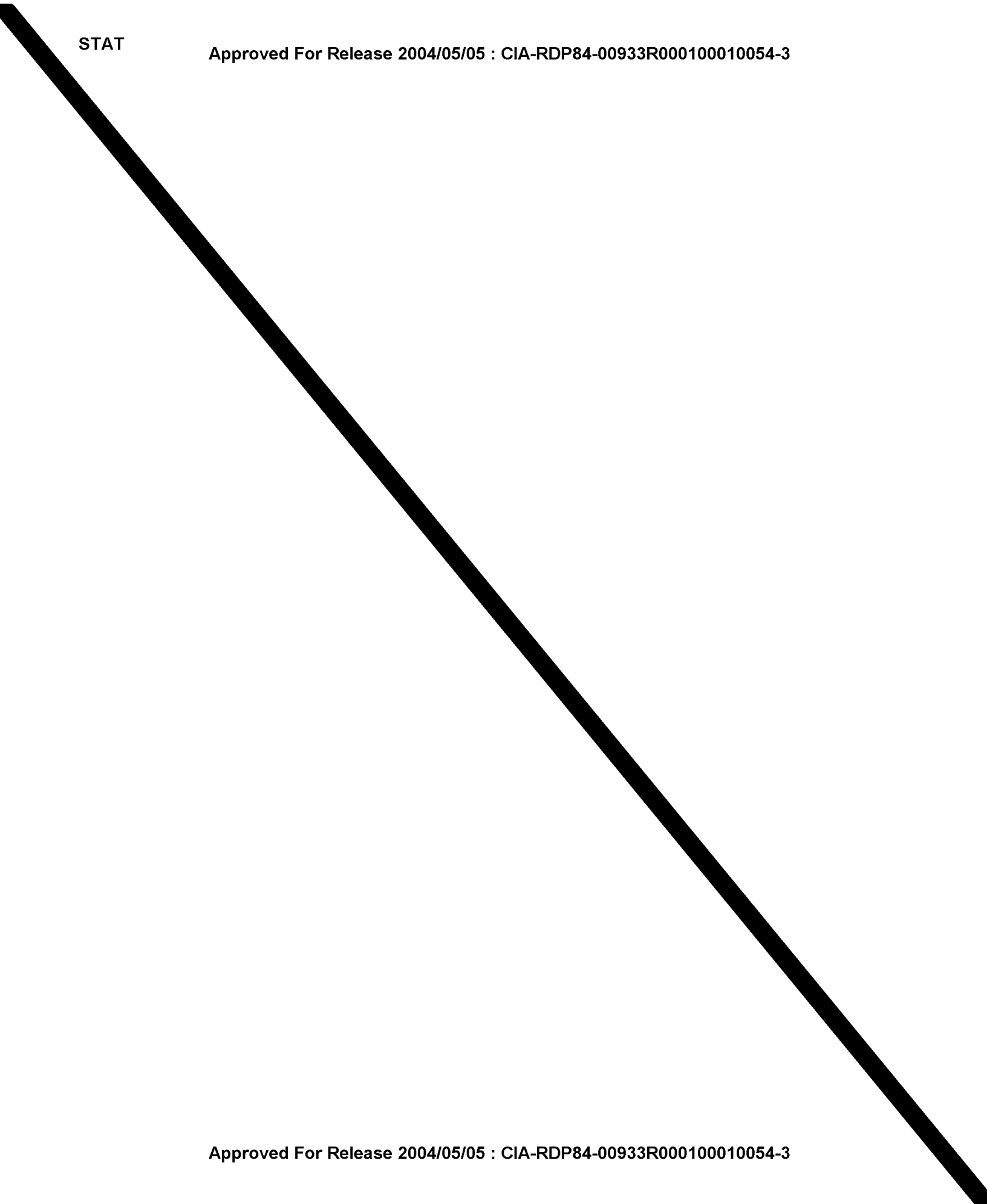
STAT

STAT [redacted] of my staff [redacted]

[redacted]

STAT

Attachments: a/s



Approved For Release 2004/05/05 : CIA-RDP84-00933R000100010054-3

It is proposed that the specifications section of FIPS PUB 71, Advanced Data Communication Control Procedures, be revised to add the following two new items:

(4) All systems shall implement the 16-bit frame check sequence (FCS) specified in American National Standard X3.66-1979, referenced above.

A 32-bit FCS may also be provided for use when it has been determined that a higher degree of error protection is necessary on a link. For a discussion of the relative merits of the 16-bit and 32-bit FCS, see FIPS PUB 78, Guideline for Implementing Advanced Data Communication Control Procedures, Section 7.8.

The equations for 32-bit FCS generation are:

$$\frac{X^{32}G(X)^k + X^kL(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$

$$FCS = L(X) + R(X) = R(X)$$

The arithmetic is modulo 2.

$$L(X) = X^{31}+X^{30}+X^{29}+X^{28}+X^{27}+X^{26}+X^{25}+X^{24}+X^{23}+X^{22}$$
$$+X^{21}+X^{20}+X^{19}+X^{18}+X^{17}+X^{16}+X^{15}+X^{14}+X^{13}+X^{12}+X^{11}+X^{10}$$
$$+X^9+X^8+X^7+X^6+X^5+X^4+X^3+X^2+X^1+1.$$

R(X) = The remainder which is of degree less than 32.

k = The number of bits represented by G(X).

P(X) = The generator polynomial $X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{2}+X^{1}+1$

G(X) = The message polynomial, which includes the contents of the address, control, and information fields, excluding the zero bits inserted for transparency (see American National Standard X3.66-1979, Section 3.7).

The generation of the remainder R(X) differs from that used in conventional (non-ADCCP) check sequence generation by the presence of the $X^k$ L(X) term in the generation equation. When the 32-bit FCS generation is by the usual shift register technique, the $X^k$ L(X) term is added in either of two ways:

a. Preset the shift register to all ones rather than to all zeros as in conventional (non-ADCCP) generation procedures. Otherwise, shift the data G(X) through the register as in conventional procedures, or,

b. Invert the first 32 bits of G(X) before shifting

into the register and shift the remaining part of G(X) through the register uninverted. This requires that G(X) contain at least 32 bits.

Whether 1 or 2 is used, the shift register contents, after shifting through G(X), are R(X). These contents are inverted bit-by-bit and transmitted as the FCS sequence.

The transmitted sequence is always (in algebraic notation): $M(X) = X^{32} G(X) + FCS$.

The received sequence will be denoted M*(X) and may differ from the transmitted sequence M(X) if transmission errors are introduced. The checking process always involves dividing the received sequence by P(X) and testing the remainder. Direct division, however, does not yield a unique remainder and it is expected that in most cases the received sequence will be modified for checking purposes by the addition of terms which will cause the division to yield such a unique remainder when M*(X) = M(X), i.e., when the frame is error free.

Two classes of checking equations are given below:

$$\frac{X^{\gamma}[M^*(X) + X^k L(X)]}{P(X)} = Q(X) + \frac{R(X)}{P(X)} \quad \text{(Equation 1)}$$

In this case, the unique remainder is the remainder of the division $X^{\gamma} \frac{L(X)}{P(X)}$

When $\gamma = 0$ the remainder is L(X) (32 ones).
When $\gamma = 32$ the remainder is $X^{31}+X^{30}+X^{26}+X^{25}+X^{24}$ $+X^{18}+X^{15}+X^{14}+X^{12}+X^{11}+X^{10}+X^8+X^6+X^5+X^4+X^3+X^1+1$.

$$\frac{X^{\gamma}[M^*(X)^k + (X + 1)\ L(X)]}{P(X)} = Q(X) + \frac{R(X)}{P(X)} \quad \text{(Equation 2)}$$

In this case, the unique remainder is always zero regardless of the value of $\gamma$.

Shift register implementation of the above equations normally use $\gamma = 32$ (pre-multiplication). When this is the case, the added term $X^k L(X)$ in Equations 1 and 2 is added by either inverting the first 32 received bits of M*(X) before shifting them through the checking register or by presetting the register to all ones and shifting all of M*(X) through normally. Thus, the receiver action on the leading portion of a frame is the same with either Equation 1 or 2.

The +1 of the term $(X^k+1)L(X)$ of Equation 2 is added by inverting the 32-bit FCS. This implies a 32-bit

storage delay by the 32-bit FCS function at the receiver since the location of the 32-bit FCS is not known until the closing flag is received.

(5) To maximize interoperability among major Federal data communication networks, while still allowing flexibility to tailor a network for efficient day-to-day use, the following features are required:

a. The W bit in the frame reject (FRMR) information field shall be set to indicate the cause of the frame rejection condition. (See American National Standard X3.66-1979, Section 7.5.3.1.)

b. Upon receiving a FRMR with the W bit set to one, a primary/combined station shall issue an appropriate mode setting command (i.e., SNRM, SARM, SABM, SNRME, SARME, or SABME) and shall not subsequently, during the same connection with the same secondary/combined station, transmit a frame containing the command or response that caused the frame rejection condition. (See American National Standard X3.66-1979, Section 7.4.1.)

It is also proposed that the cross-index section of FIPS PUB 71 be revised to add the following new items:

(c) FIPS PUB 78, Guideline for Implementing Advanced Data Communication Control Procedures.

(d) International Standard 3309: Data Communications - High-level Data Link Control Procedures - Frame Structure.

(e) International Standard 4335: Data Communications - High-level Data Link Control Procedures - Elements of Procedures.

(f) Addendum 1 to International Standard 4335: Data Communications - High-level Data Link Control Procedures - Elements of Procedures.

(g) Addendum 2 to International Standard 4335: Data Communications - High-level Data Link Control Procedures - Elements of Procedures.

(h) International Standard 6159: Data Communications - High-level Data Link Control Procedures - Unbalanced Classes of Procedure.

(i) International Standard 6256: Data Communications - High-level Data Link Control Procedures - Balanced Class of Procedure.

(j) CCITT Recommendation X.25: Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks.

(k) CCITT Recommendation X.75: Terminal and Transit Call Procedures and Data Transfer Systems on International Circuits Between Packet-Switched Data Networks.